Remarks

Applicants respectfully request reconsideration of this application as amended. Claims 1-8, 10-17, 19-26, 28, 29 and 31 have been amended. No claims have been cancelled. Therefore, claims 1-33 are presented for examination.

Claims 1-33 stand rejected under 35 U.S.C. §102(e) as being anticipated by Redlich et al. (U.S. Patent No. 7,140,044). Applicants submit that the present claims are patentable over Redlich.

Redlich discloses a method for securing data in a computer system that includes establishing a group of security sensitive words, characters, icons, data streams or data objects, filtering the data input from a data input device and extracting the security sensitive data. The extracted data is separated from the remainder data and is separately stored. In one embodiment on a personal computer (PC) system, the extracted data and the remainder or common data is stored in different, distributed memory segments. In a network implementation, the extracted data may be stored in one computer and the remainder or common data may be stored in another computer. In a client-server implementation, the server may direct storage of the extracted data to a different location than the remainder data, either on the server or on a further memory system (computer) interconnected to the server or on the client computer and in distributed memory segments. A map may be generated by a software module or sub-system indicating the location of the extracted data and the remainder data in the network. The filter may be destroyed (via a deletion routine) or may be retained for future use by the user. If retained, encryption is preferred. The map may be stored on the client computer or the user's PC or may be stored on the server. Copies of the map may be removed (deleted) from the user's PC or the client computer. The map may be encrypted. The extracted data and/or the remainder data may be removed (deleted or scrubbed) from the originating computer. Encryption can be utilized to further enhance the security levels of the system. All transfers of the filter between the client to the server may be encrypted, and all data (whether extracted data or remainder data) may be encrypted prior to storage in the distributed memory. Any transfer of extracted data or remainder data or maps or filters may include an encryption feature. Reconstruction of the data is permitted only in the presence of a predetermined security clearance. A plurality of security clearances might be required which would enable a corresponding plurality of reconstructing users to view all or portions of the data. Persons with low level security clearance would only be permitted to have access to low level extracted data (low level security sensitive data) and the common data. Persons with high level security clearances would be permitted access to the entire document reconstituted from the extracted data and the remainder data. See Redlich at col. 6, ll. 60 – col. 7, ll. 39.

Claim 1 of the present application recites generating check data to be stored in storage based upon one or more portions of encrypted write data. Applicants submit that nowhere in Redlich is there disclosed a process of generating check data to be stored in storage, and particularly, no generated check data based upon encrypted write data. Therefore, claim 1 is patentable over Redlich.

Claims 2-4 depend from claim 1 and include additional features. Thus, claims 2-4 are also patentable over Redlich.

Independent claims 10, 19 and 28 disclose limitations similar to those in claim 1. Accordingly, claims 10, 19 and 28, and their respective dependent claims, are patentable over Redlich for the reasons discussed above with respect to claim 1.

Claim 5 recites retrieving one or more respective portions of encrypted data from a plurality of storage devices and decrypting, based upon at least one key, one or more respective portions of the encrypted read retrieved data. Applicants submit that Redlich fails to disclose retrieving encrypted data from a plurality of storage devices and decrypting, the retrieved encrypted data based upon at least one key. Therefore, claim 5 is patentable over Redlich. Since claims 6-9 depend from claim 5 and include additional features, claims 6-9 are also patentable over Redlich.

Independent claims 14, 23 and 31 disclose limitations similar to those in claim 5. Accordingly, claims 14, 23 and 31, and their respective dependent claims, are patentable over Redlich for the reasons discussed above with respect to claim 5.

Applicants submit that the rejections have been overcome and that the claims are in condition for allowance. Accordingly, applicants respectfully request the rejections be withdrawn and the claims be allowed.

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: 4/23/07

Mark L. Watson
Reg. No. 46,322

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1026
(303) 740-1980